UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/756,904	01/14/2004	Marc A. Boulanger	RPS920030037US1	3081

45211 7590 11/09/2007

Robert A. Voigt, Jr.
WINSTEAD SECHREST & MINICK PC
PO BOX 50784
DALLAS, TX 75201

EXAMINER	
SCHMIDT, KARI L	
ART UNIT	**PAPER NUMBER**
2139	
MAIL DATE	**DELIVERY MODE**
11/09/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

mN

Office Action Summary	**Application No.** 10/756,904	**Applicant(s)** BOULANGER ET AL.
	Examiner Kari L. Schmidt	**Art Unit** 2139

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 27 August 2007.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-21 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-21 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 14 January 2007 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Notice to Applicant

This communication is in response to the amendment filed on 08/23/2007. Claims 1-21 remain pending. Further new grounds of rejection have been established for claims 12-17 and 20. Same grounds of rejection are maintained for claims 1-11 and 18-19, and 21. This action is made non-final.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-11, and 18-19 and 21 are rejected under 35 U.S.C. 102(e) as being anticipated by Shanklin et al. (US 6,578,147).

<u>Claims 1 and 6 and 21</u>

Shanklin discloses a method for rapid intrusion detection for network communication comprising the steps of:

receiving packets of network data in a network processor coupled to a network fabric (col. 3, lines 10-18: "receives and sends data in "packets" which are switched between network segments by router");

forwarding routed network data to the network fabric; and coupling selected data from the network data to a parallel pattern detection engine (PPDE), for comparing the selected data in parallel to M sequences of pattern data stored in the PPDE and generating a match output signal when at least one of the M sequences of pattern data compares to a portion of the selected data (col. 2, lines 59 – col. 3, line 3: "each sensor is identical to the other sensors and is capable of performing the same intrusion detection processing. The sensors operate in parallel, and analyze packets to determine if any packet or series of packets has a signature that matches on of a collection of known intrusion signature..").

Claims 2, 7, and 8

Shanklin discloses the method of claim 1, further comprising the steps of: storing N intrusion signatures in the M PUs sequences of pattern data with corresponding identification (ID) data used to identify which of the N intrusion signatures is detected (col. 6, lines 25-46: "each senor has a unique IP address" and col. 1, lines 50-60: "one known pattern of unauthorized access is associated with "IP spoofing" whereby an intruder sends a message is from a trusted port. To engage in IP spoofing, the intruder must first use a variety of techniques to find a IP address of a trusted port and must then modify the packet headers so that it appears that the packets are coming from that port. This activity result in a signature that can be detected when matched to a previously stored signature of the same activity"); and storing action code indicating action to take in response to detecting a particular one of the N intrusion signatures ("col. 4, lines 54-61: "sensor contains a detection engine... the senor also analyzes each packet's relationship to adjacent and related packets in the data stream and if the analysis indicates misuse the senor may act autonomously to take action, such as disconnection..").

Claims 3 and 9

Shanklin discloses the method of claim 2, further comprising the steps of:

analyzing the packets of network data for validity thereby generating valid packets of network data as the selected data (col. 6, lines 9-24: "session analyzer which stores information used to detect signatures from different packets in the same session... For example, a first sensor might receive a packet indicating a signature that would be comprised of different packets from the same session...");

comparing the selected data to the store N intrusion signatures and generating, at network data speed, a pattern compare signal and particular ID data when a particular one of the N intrusion signatures is detected (col. 2, lines 59 – col. 3, lines 1-3: " sensors operate in parallel and analyze packets to determine if any packet or seris of packets has a signature that matches on of a collection of known intrusion signatures... invention provides an easily scalable solution to providing an intrusion detection system whose ability to perform signature analysis can keep up with high speed networks; col. 7, lines 29-39) ; and

executing the action code corresponding to the particular one of the N intrusion signatures detected ("col. 4, lines 54-61: "sensor contains a detection engine... the senor also analyzes each packet's relationship to adjacent and related packets in the data stream and if the analysis indicates misuse the senor may act autonomously to take action, such as disconnection..").

Claim 4 and 10

Shanklin discloses the method of claim 3, wherein the PPDE comprises:

an input/output (I/O) interface for coupling data into and out of the PPDE;

M' processing units (PUs), each of the M PUs having compare circuitry for comparing each of the sequence of input data to pattern data stored in each of the M PUs and generating a compare output, wherein an address pointer selecting the pattern data in each of the M PUs is modified in response to a logic state of the compare output and an operation code stored with the pattern data;

an input bus for coupling the sequence of input data to each of the M PUs in parallel;

an output bus coupled to the I/O interface for sending output data to the I/O interface;

control circuitry coupled to the I/O interface and coupling control data on a control data bus and identification (ID) on an ID bus to each of the M processing units; and

ID selection circuitry for selecting a match ID from ID data identifying the M PUs in response to a pattern match signal and match mode data, wherein the match ID and match data corresponding to the match ID are saved in a temporary register as the output data (Figure 4 and col. 7, lines 1-27: "a switch having internal intrusion detection sensors.. packets are forwarded by switch based on destination address and the operation of switch is such that its control unit ensures that only packets having a certain address are output from the port...").

Claim 5, 11, and 18-19

Shanklin discloses the method of claim 3, wherein the PPDE further comprises cascade circuitry coupled from each of the M PUs to one or more adjacent PUs within the M PUs for selectively coupling chain data between one or more groups of two or more adjacent PUs selected from the M PUs in response to the control data (Figure 4, col. 4, lines 54-61: "sensor contains a detection engine, which examines each packet incoming to the senor including its header and payload. The sensor also analyzes each packet's relationship to adjacent and related packets in the data stream..." col. 4, lines 54-61: "sensor contains a detection engine... the senor also analyzes each packet's relationship to adjacent and related packets in the data stream and if the analysis indicates misuse the senor may act autonomously. to take action, such as disconnection..").

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 12-17 and 20 rejected under 35 U.S.C. 103(a) as being unpatentable over Shanklin et al. (US 6,578,147) in view of Alles (US 4,112,258).

Claims 12-17 and 20

Shanklin discloses a device with complex internal structure in printed circuit boards which are connected to one or more sensors with various buffers and control structures (see at least, col. 7, lines 7-19).

Shanklin fails to disclose input/output buffer, registers, multiplexer, bus connectors, registers, and clock control cycles.

However, Alles discloses input/output buffers (see at least, col. 2, lines 8-16), registers (col. 11, lines 6-26 and 43-65), multiplexer (col. 11, lines 6-26 and 43-65), bus connectors (see at least, col. 8, 18-36), control clock cycles (see at least, col. 2, lines 8-16). The examiner further notes that it would be obvious to modify any circuitry to perform a given method as defined by claims 1-5.

The examiner takes the position that it would have been obvious to one of ordinary skill in the art to modify the teachings of Shanklins intrustion detection system and advanced control structures and circuity for handling parallel intrusion detection to include well known discloses input/output buffers, registers, multiplexer, bus, and control clock cycles as taught by Alles. One of ordinary skill in the art would have been motivated to combine the teachings in order to include a digital complex switching arrangement to efficiently handle data input threw a switch (see at least, col. 1, lines 10-30).

Response to Arguments

Applicant's arguments filed 8/23/2007 with respect to claims 1-11, and 18-19 and 21 have been fully considered but they are not persuasive.

With respect to claim 1 and 6, the applicant argues that Shanklin does not disclose **receiving packets of network data in a network processor coupled to a network fabric** and **forwarding routing network data to the network fabric** and **coupling selected data from the network data to a parallel pattern detection engine (PPDE), for comparing the selected data in parallel to M sequences of pattern data stored in the PPDE and generating a match output signal when at least one of the M sequences of pattern data compares to a portion of the selected data.**

The examiner disagrees. The examiner notes that the Shanklin reference has been read with the broadest reasonable interpretation. Further the examiner notes that exact language is not necessary for an interpretation to meet a limitation of a claim. With respect to the arguments of claims 1 and 6, the examiner notes that Shanklin discloses **receiving packets of network data in a network processor coupled to a network fabric** (see at least, col. 3, lines 10-18 and col. 3, lines 30-39). The examiner notes that a "inspects packets incoming from the external network to determine which should be forwarded to the local network" would be receiving packets of network data in a network processor coupled to a network fabric. The examiner notes that Shanklin discloses **forwarding routing network data to the network fabric** (see at least, col. 3, lines 10-18 and col. 3, lines 30-39). The examiner notes that "packets originating in the local network are inspected to determine whether they are to be forwarded to the external network. The examiner notes that Shanklin discloses **coupling selected data from the network data to a parallel pattern detection engine (PPDE), for comparing the selected data in parallel to M sequences of pattern data stored in the PPDE and generating a match output signal when at least one of the M sequences of pattern data compares to a portion of the selected data** (see at least, col. 4, lines 44-67). The examiner notes that a sensor contains a detection engine, which examines each incoming packet to analyze each packet to determine if the packet is safe for the network. Further the examiner notes that the sensors work in a parallel detection manner in order to match the incoming packet data to the signature analysis the fields of the packet for possible intrusion (see at least, col. 3, lines 59-67 and col. 4, lines 44-67 through col. 5, lines 1-11). The examiner notes that the broadest interpretation of Shanklin reads on the limitations found in claim 1 and 6, therefore this argument is not persuasive.

With respect to claims 2, 7 and 8, the applicant argues that Shanklin does not disclose **storing N intrusion signatures in the M PUs sequences of pattern data with corresponding identification (ID) data used to identify which of the N intrusion signatures is detected** and **storing action code indicating action to take in response to detecting a particular one of the N intrusion signatures.**

The examiner disagrees. The examiner notes that the Shanklin reference has been read with the broadest reasonable interpretation. Further the examiner notes that exact language is not necessary for an interpretation to meet a limitation of a claim. With respect to the arguments of claims 2, 7, and 8, the examiner notes that Shanklin discloses storing **N intrusion signatures in the M PUs sequences of pattern data with corresponding identification (ID) data used to identify which of the N intrusion signatures is detected** and **storing action code indicating action to take in response to detecting a particular one of the N intrusion signatures** (see at least, col. 3, lines 59-67 and col. 4, lines 44-67 through col. 5, lines 1-11). The examiner notes that the sensor contains a detection engine which examines incoming packets and analyzes the incoming packet headers for intrusion signatures further if a possible intrusion is found the sensor will act in an autonomous manner to take action against said intrusion. The examiner notes that the broadest interpretation of Shanklin reads on the limitations found in claim 2, 7, and 8 therefore this argument is not persuasive.

With respect to claims 3 and 9, the applicant argues that Shanklin does not disclose **comparing the selected data to store N intrusion signatures and generating, at network data speed, a pattern comparing signal and particular ID data when a particular one of N intrusion signatures is detected.**

The examiner disagrees. The examiner notes that the Shanklin reference has been read with the broadest reasonable interpretation. Further the examiner notes that exact language is not necessary for an interpretation to meet a limitation of a claim. With respect to the arguments of claims 3 and 9 the examiner notes that Shanklin discloses **comparing the selected data to store N intrusion signatures and generating, at network data speed, a pattern comparing signal and particular ID data when a particular one of N intrusion signatures is detected** (see at least, col. 3, lines 59-67 and col. 4, lines 44-67 through col. 5, lines 1-11 and col. 6, lines 9-11). The examiner notes that the sensor contains a detection engine which examines incoming packets and analyzes the incoming packet headers for intrusion signatures further stores information used to detect signatures from different packets within the same session. The examiner notes that the broadest interpretation of Shanklin reads on the limitations found in claim 3 and 9 therefore this argument is not persuasive.

With respect to claims 4 and 10, the applicant argues that Shanklin does not disclose **executing the action code correspond to the particular one of N intrusion signatures detected** and **an I/O interface for coupling data into and out of the**

PPDE which compares M PUs input data to generate a compare output which is matched to an ID to identify the M PUs pattern match.

The examiner disagrees. The examiner notes that the Shanklin reference has been read with the broadest reasonable interpretation. Further the examiner notes that exact language is not necessary for an interpretation to meet a limitation of a claim. With respect to the arguments of claims 4 and 10, the examiner notes that Shanklin discloses **executing the action code correspond to the particular one of N intrusion signatures detected** and **an I/O interface for coupling data into and out of the PPDE which compares M PUs input data to generate a compare output which is matched to an ID to identify the M PUs pattern match** (see at least, col. 3, lines 59-67 and col. 4, lines 44-67 through col. 5, lines 1-11 and col. 6, lines 9-14). The examiner notes that a session analyzer stores information used to detect signatures from different packets in the same session and further receives packets from further sensors which processes information to determine the state of the packet A, and then these states can be acted upon (e.g. compared) and the session anaylizer can act accordingly. The examiner notes that the broadest interpretation of Shanklin reads on the limitations found in claim 4 and 10 therefore this argument is not persuasive.

With respect to claim 5, 11, 18 and 19, the applicant argues that Shaklin does not disclose **wherein the PPDE further comprises cascade circuitry coupled from of the M PUs to one or more adjacent PU's within the M PU's for selectively coupled**

chain data between one or more groups of two or more adjacent PUs selected from the M PU's in response to the control data.

The examiner disagrees. The examiner notes that the Shanklin reference has been read with the broadest reasonable interpretation. Further the examiner notes that exact language is not necessary for an interpretation to meet a limitation of a claim. With respect to the arguments of claims 5, 11, 18 and 19, the examiner notes that Shanklin discloses **wherein the PPDE further comprises cascade circuitry coupled from of the M PUs to one or more adjacent PU's within the M PU's for selectively coupled chain data between one or more groups of two or more adjacent PUs selected from the M PU's in response to the control data** (see at least, Figure 3-6 and col. 3, lines 59-67 and col. 4, lines 44-67 through col. 5, lines 1-11 and col. 6, lines 9-14 and lines 25-46). The examiner notes the IDS sensors are configured in a series that are adjacent to on another and further data can be load balanced between sensors by encapsulating incoming packets. Further the examiner notes that all packets for a particular session are delivered to the same one of sensors and the load balancer operates by inspecting each packet and retransmitting them to the appropriate sensor (see at least, col. 7, lines 53-59). The examiner notes that the broadest interpretation of Shanklin reads on the limitations found in claim 5, 11, 18 and 19, therefore this argument is not persuasive.

With respect to claim 12, 13, and 14, the applicant argues that Shanklin fails to disclose a **multitude of buffers**.

The examiner disagrees. The examiner notes that the Shanklin reference has been read with the broadest reasonable interpretation. Further the examiner notes that exact language is not necessary for an interpretation to meet a limitation of a claim. With respect to the arguments of claims 12, 13, and 14, the examiner notes that Shanklin discloses a multitude of buffers (see at least, col. 7, lines 15-20). The examiner notes that the device has a complex internal structure with various buffers and control structures. The examiner notes that the broadest interpretation of Shanklin reads on the limitations found in claim 12, 13, and 14, therefore this argument is not persuasive.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kari L. Schmidt whose telephone number is 571-270-1385. The examiner can normally be reached on Monday - Friday: 7:30am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KS

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100